**Pearson BTEC Level 3 Nationals Diploma, Extended Diploma**

**Window for supervised period:**
**Monday 4 January 2021 – Friday 22 January 2021**

Supervised hours: 5 hours | Paper Reference **20158K**

# Information Technology

## Unit 11: Cyber Security and Incident Management

**Part A**

**You must have:**
Risk_Assessment.rtf
Security_Plan.rtf

## Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

## Information

- The total mark for this Part is 43.

*Turn over* ▶





W 6 7 6 9 9 A

Pearson

## Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

**Part A** and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

**Maintaining Security**

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

**Outcomes for Submission**

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

**[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A**

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder, using the file names listed.

**Activity 1:** activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

**Activity 2:** activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

**Activity 3:** activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 26 January 2021.

**Instructions for Learners**

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

**Part A** materials must not be accessed during the completion of **Part B**.

**Outcomes for Submission**

You must create a folder to submit your work. The folder should be named according to this naming convention:

**[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A**

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within your folder, using the file names listed.

**Activity 1:** activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

**Activity 2:** activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

**Activity 3:** activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

**BLANK PAGE**

**Set Task Brief**

**Caelcabben Manor Estate**

Caelcabben Manor Estate (CME) occupies a valley in southern England. CME has been owned by the Caelcabben family since the manor house was built in the 1300s. The current owner is Andrew Caelcabben.

Like many other historic homes, the manor house and estate are run as a tourist attraction. CME offers:

1. holiday chalets
2. tours of the manor house
3. a souvenir shop in the manor house
4. access to the gardens
5. a cafe
6. a venue for events such as shows and weddings.

The manor house also contains:

- the estate office
- an apartment where Andrew lives.

**Figure 1** shows the area around the manor house. There is a public road to the west and a fence on the other three sides. The land beyond the fence rises into steep hills. The space to the south is used for events. The two buildings there contain offices, toilets, showers and other facilities. These buildings are only open when there are events.

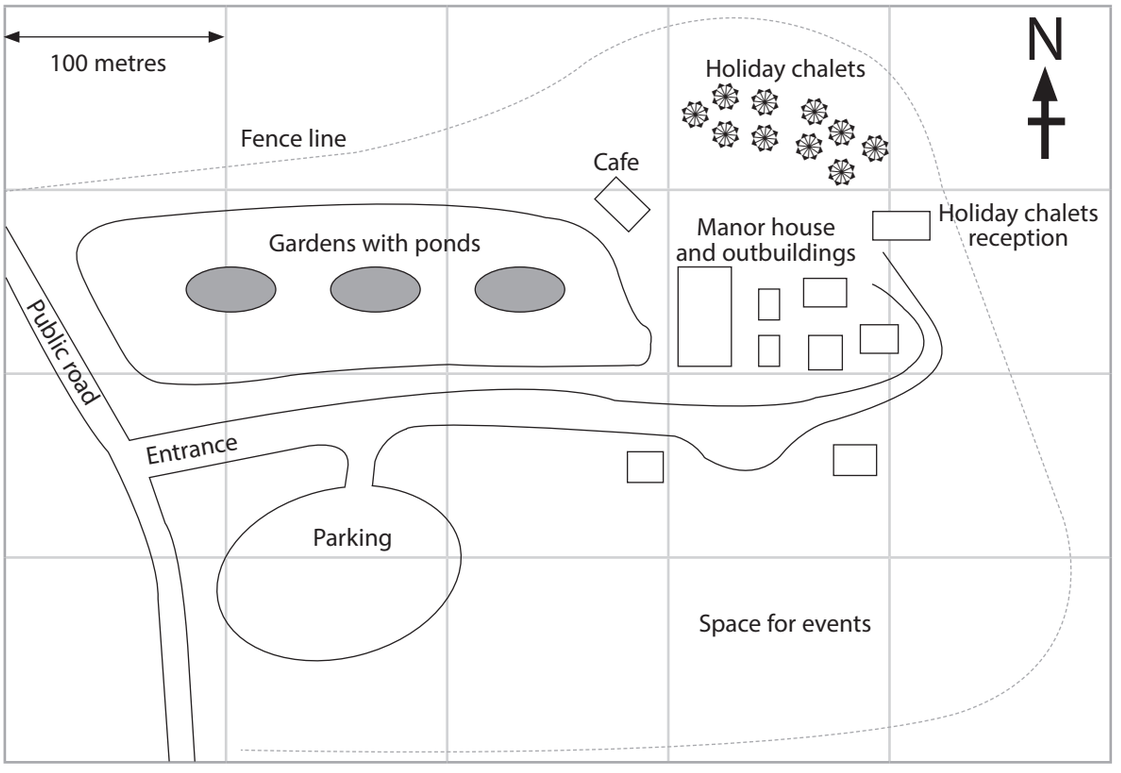


**Figure 1**

Last year fibre broadband internet access became available in the area and Andrew has decided to improve and extend the IT facilities at CME. **Figure 2** shows the **current** system.

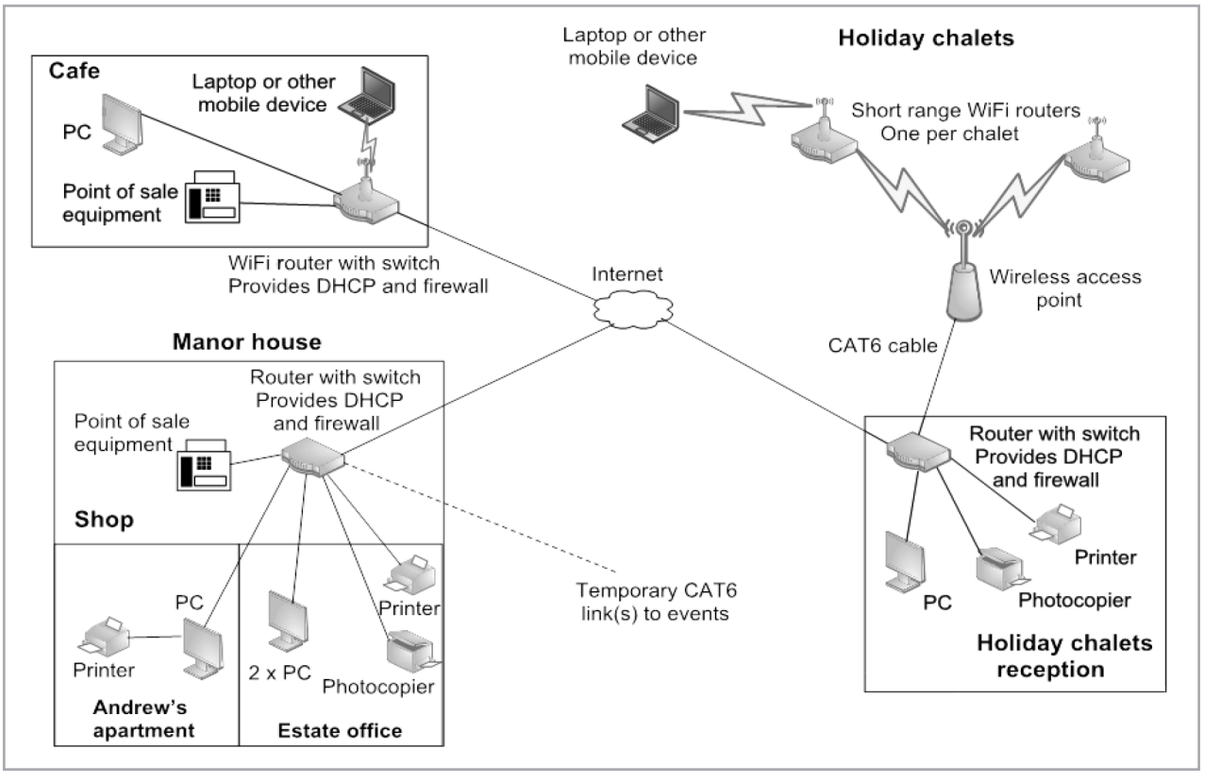


**Figure 2**

Estate staff communicate via radio transceivers. These have a theoretical range of 10 km but, in reality, the hills surrounding the estate block the signal.

Andrew has many years of experience in estate management but considers himself an IT user rather than an IT specialist. He uses CME's administrative staff for most computing tasks.

The CME staff include a Technical Manager, Joanne Reedsman, and two electricians. They look after all electrical items on the estate, including the IT system. They can deal with minor IT problems but call in outside contractors when necessary.

Andrew and Joanne have discussed the requirements of the new IT system and have made a provisional plan. They have hired you to look at the plan and advise on cyber security and incident management.

**Development plan**

At a meeting with Andrew and Joanne you establish that:

1 All the current systems will be combined into a single CME network

2 Internet access will be via a router in the estate office

3 The router will be a business-grade machine with an integrated hardware firewall

4 Each chalet will have a networked smart TV and a data socket

5 The area in and around the chalets will have free high speed WiFi broadband

6 WiFi access will cover all the other buildings plus the gardens immediately in front of the cafe. This will be free but with limited bandwidth per connection

7 Joanne is concerned about the available bandwidth, even with a fibre connection. She wants to restrict the high speed WiFi broadband to chalet occupants only

8 CAT6 cabling will be extended to the buildings in the events area to provide WiFi coverage in that area when needed

9 Event WiFi / network connections must be isolated from the free WiFi

10 CME staff must be able to monitor the traffic on all of the WiFi systems

11 Estate staff will continue to use radio transceivers for communication

12 The CME network servers will run Ubuntu (Linux)

13 One server will act as the DHCP and file server

14 One server will act as the web and email server

15 Both servers will be supplied and configured for their roles by a local contractor

16 Andrew wants a robust backup system. He is considering using RAID 1 on the two servers and a network attached storage device to store recovery files and periodic disk images

17 Guests must not be able to access any of the estates systems except the free WiFi.

## Part A Set Task

**You must complete ALL activities in the set task.**

**Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.**

Andrew has hired you to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

**Activity 1: Risk assessment of the networked system**

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

**(Total for Activity 1 = 8 marks)**

**Activity 2: Cyber security plan for the networked system**

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

**(Total for Activity 2 = 20 marks)**

**Activity 3: Management report justifying the solution**

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

**(Total for Activity 3 = 12 marks)**

**TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS**
**TOTAL FOR PART A = 43 MARKS**